计算机系统信息隐藏反取证技术①

李佟鸿, 王 宁, 刘志军

(湖北警官学院, 武汉 430032)

摘 要: 研究了现代计算机系统信息隐藏的各种可能方式. 运用 HPA 和 DCO、隐藏分区等技术分析了磁盘驱动的数据隐藏, 运用簇分配、Slack 空间等技术分析了 NTFS 文件系统的各种信息隐藏方法, 以及各种方法可能的检测手段. 分析各种隐藏技术作为计算机反取证手段, 给计算机取证带来的巨大影响.

关键词: 信息隐藏; 反取证; 隐藏分区; 簇分配; Slack 空间; NTFS 文件系统

Data Hiding and Anti-Forensic on Modern Computer System

LI Tong-Hong, WANG Ning, LIU Zhi-Jun

(Hubei University of Police, Wuhan 430032, China)

Abstract: This paper discusses some of the possible ways to hide data on modern computer systems. Using HPA and DCO, hidden partition and other technical analysis of the disk drive data hidden. Using the cluster distribution, Slack space and so on technical discusses some of the methods that can be used to hide data in NTFS and analysis techniques that can be used to detect and recover hidden data. The exploration of the different hiding technology can be used as computer anti-forensics means, to the great impacts of computer forensics.

Key words: data hiding; anti-forensic; hidden partition; cluster distribution; Slack space; NTFS

1 引言

随着计算机取证技术的发展, 计算机反取证(Computer Anti-Forensic)技术也正悄然兴起, 反取证针对计算机取证过程的各个阶段, 破坏电子证据的调查、保护、收集、分析和法庭诉讼, 减少被获取的证据数量, 降低所获取证据的质量. 这对取证技术的发展形成了严峻的挑战.

常见的反取证技术主要有数据擦除、数据隐藏、数据加密、网络源反追踪、内核级 Rootkit、针对计算机取证工具缺陷进行攻击等技术手段. 其中, 数据隐藏是计算机反取证最主要手段之一. 数据隐藏通常有非物理形式的数据隐藏和物理形式的数据隐藏[1]. 非物理形式的数据隐藏是通常意义上的信息隐藏, 主要包括数据加密、隐写术和数字水印; 物理形式的数据隐藏主要是与计算机存储设备和操作系统有关的数据隐藏. 这里主要探讨物理形式的数据隐藏. 本文主要研究了现代计算机系统各种数据隐藏方法和策略, 以及数据隐藏反取证技术对计算机取证造成的影响.

2 计算机硬件信息隐藏

2.1 HPA 和 DCO 数据隐藏

(1) 主机保护区域 HPA

在 ATA-5 协议被确立以后, 硬盘引入了主机保护区域(Host Protected Area 即 HPA)技术, 通过用 ATA 命令直接把硬盘后部的一块区域保护起来, 用于存储数据和配置文件, 操作系统和 BIOS 都无法读取该区域[2]. 如果一块 120GB 的硬盘设置了 10GB 的“隐藏保护区域”, 那么在 BIOS 也只能检测到 110GB. 硬盘未被保护的区域, 可进行正常的读写、分区、格式化, 而不会对 “隐藏保护区域”内的数据有任何影响. 然而, 也有一些工具可以对 HPA 进行修改, 以实现数据隐藏. 一旦能够进入这些受保护的区域, 就可以隐藏大量的数

① 基金项目:国家社会科学基金项目(12CFX053);公安部应用创新项目(2010YYCXHBST061,2011YYCXHBST068);湖北省自然科学基金(2011CDB086);教育部人文社会科学研究青年基金(09YJCZH037,11YJCZH168);湖北省教育厅科学技术研究项目(Q20114201)

收稿时间:2012-10-13;收到修改稿时间:2012-11-19

据，这些区域往往不会被取证分析员所重视，部分取证软件还不能有效获取该区域隐藏数据.

(2) 设备配置覆盖 DCO

设备配置覆盖(Device Configuration Overlay, DCO)是硬盘驱动器(HDD)另一个隐藏区域，在 ATA-6 标准中首次引入, DCO 比 HPA 具有更强隐藏数据的能力[2]. 设计 DCO 的目的是允许系统供应商购买来自不同厂商的硬盘驱动器，可能大小不同，然后配置所有硬盘驱动器具有相同的扇区数.

如果硬盘驱动支持 HPA/DCO，则二者可单独存在或同时存在，如图 1 所示，1.5TG 的磁盘驱动，HPA 占 500G，或 1.5TG 磁盘驱动, HPA 和 DCO 各 250G.

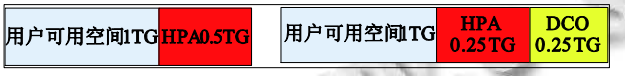

图 1　只含有 HPA 或同时含有 HPA/DCO 的磁盘驱动

(3) 数据隐藏分析

运用相关工具可以创建和修改硬盘驱动器的 HPA/DCO. 如 HDAT2、SETMAX、Feature Tool、MHDD 等. 如图 2 所示，使用 MHDD 将一个 200G 的 Seagate 硬盘改为 100G.

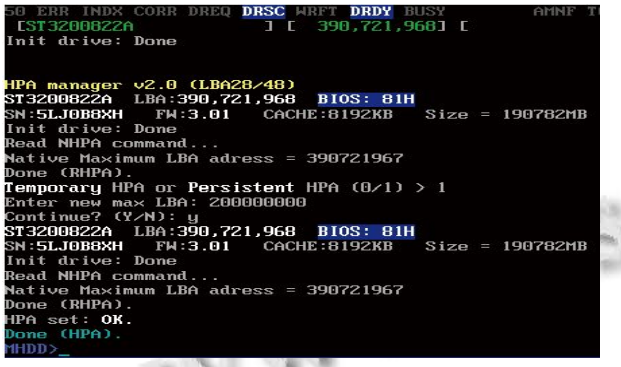

图 2　创建 HPA

创建或控制一个 HPA/DCO 隐藏数据，需要如下几步：首先用磁盘编辑工具将需要隐藏的文件拷贝到所在磁盘分区的末端；其次在需隐藏文件所在区域创建一个 HPA，所占空间大小可以根据需要任意确定；最后消除源文件空间指向新文件空间的引用，这样在磁盘驱动器上就可以拥有一个隐藏文件. 如果不用针对 HPA 区域的专门软件或硬件工具，是不会发现该文件. 对运用 HPA/DCO 实施数据隐藏的取证分析工具，目前有很多，如 The Sleuth Kit、The ATA Forensics Tool、EnCase 等软件工具，还有硬件工具如 Forensic Ultradock v4、Forensic RTX 等.

2.2 隐藏分区

隐藏分区，就是在一般条件下，不显示也不能直接使用的硬盘的部分空间，一般不能访问. 一些品牌机如联想的笔记本等默认出厂给自己划出一个隐藏分区，以便存储一些系统启动或类似一键恢复的主要文件，并提供启动入口. Windows7 操作系统在全新安装或者是对分区格式化的时候，也会预留一定的空间作为启动引导文件存放的分区，该分区为隐藏分区.

另外，也可以使用相关工具设置隐藏分区. 如 DiskGenius 可以实施分区隐藏和隐藏分区分析. 笔者将某一磁盘分区隐藏，用 encase4.0 分析验证，看不到隐藏的文件，如图 3 所示:

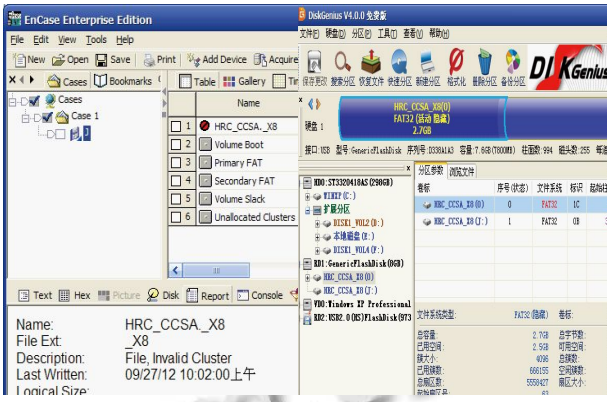

图 3　将一分区隐藏并用 encase4.0 分析查看

如果运用技术手段将数据隐藏在隐藏分区中，将是有效的反取证手段. 所以取证分析员在取证分析的时候，需要运用多种手段，全面考虑证据获取的全面性和完整性.

2.3 残留空间(Slack Space)信息隐藏

磁盘上的残留空间主要有卷残留(Volume Slack)和文件系统残留(File System Slack). 卷残留是文件系统所在的分区，介于文件系统末端和分区末端之间的未使用的空间. 文件系统残留是文件系统末端，没有分配给任何簇的未使用的空间[3]. 出现卷残留和文件系统残留的原因是分区不是簇的整数倍造成的. 例如，在一个分区里有 10001 个扇区，前 10000 个扇区分成 2500 个簇，每簇有 4 个扇区，那么，最后一个扇区就剩下来，成为文件系统残留.

在卷残留隐藏的数据量是不受限制的，因此，嫌疑人可以简单的修改卷残留的大小来隐藏更多的数据. 而在文件残留隐藏数据要受到簇的大小限制，比如，文件系统一个簇有八个扇区，在这个文件系统残留里所能隐藏的最大数据量是 7 个扇区的容量.

Slack 空间隐藏数据，是文件系统及整个计算机系统存储能力的产物. Slack 空间数据隐藏技术，充分利用了格式化存储介质的物理特性来隐藏数据. 采用该技术进行数据隐藏有双重优点：主机或者载体文件不受任何影响，且不会影响整个数字系统的正常运行. 其原因在于隐藏数据对于操作系统和文件管理器来说是透明的. 向 Slack 空间写入数据实施数据隐藏，也是反取证技术的重要手段之一，犯罪分子可以向该区域隐藏各种信息，如各种病毒、木马以及进行犯罪的软件工具等.

检测 Slack 空间的隐藏数据，简单的方法可以使用 Windows 命令行工具 chkdsk 来分析文件系统，复杂的就需要借助专门的工具来实现，如 Guidance 公司的 Encase 软件, NTI 公司的 GetSlack 软件等工具，支持对这些空间的证据的收集和分析.

3 计算机NTFS文件系统数据隐藏

NTFS 文件系统是目前微软操作系统的标准文件系统，在 NTFS 文件系统中有很多隐藏数据的方法[4]. 在这一部分，我们主要讨论常见的数据隐藏方法以及隐藏数据的检测手段.

3.1 NTFS 数据隐藏标准

从犯罪嫌疑人的角度来说，一个好的 NTFS 数据隐藏技术应该符合如下标准：一是正常的系统工具(如 chkdsk 等)检查不出任何错误；二是隐藏的数据不被改写或被改写的可能性非常低；三是正常的用户不能发现隐藏的数据；四是该技术可以储存一定数量的隐藏数据[5].

3.2 标注坏簇信息隐藏

在硬盘中，无法被正常访问或不能被正确读写的扇区，都称为坏扇区(Bad sector). 在 NTFS 主文件表(MFT, Master File Tab)中，有一个坏簇列表文件($BadClus)，它记录了磁盘上该卷中所有的损坏的簇号，防止系统对其进行分配使用. 把要隐藏的文件所在的簇标记为坏簇，就是把这些簇的“指针”添加到 $BadClus 的数据运行列表中，就可以实现该文件的隐藏，用这种方法隐藏的数据的大小是不受限制的. 犯罪嫌疑人可以简单地分配更多的簇至 $BadClus，用它来隐藏数据，而不必担心隐藏数据遭到破坏[5].

3.3 分配给文件多余的簇信息隐藏

这种信息隐藏的方法，是使用分配给文件多余的簇来隐藏数据. 比如，一个文件有 10752 比特大小，NTFS 文件系统需要分配给它 3 个簇，每簇 8 个扇区，但嫌疑人可以给这个文件分配更多的簇，以实现数据隐藏的目的. 用这种方式隐藏数据的大小也不受限制，因为嫌疑人可以根据自己的需要，分配给文件多余的簇. 使用这种隐藏方式，有一个弊端，就是存储的文件大小不能改变，一旦文件的容量增加，隐藏数据就被覆盖或丢失. 维持存储文件的稳定不变，是维持这种信息隐藏的前提.

对于这种数据隐藏方法的检测，可以使用 Windows 命令行工具 chkdsk 来分析. 目前还没有专门的工具实现这个自动检测过程.

3.4 文件 Slack 空间信息隐藏

文件 Slack 空间就是文件有效数据的结尾位置，到最后一个数据块的最末端位置之间的存储空间. Wi-ndows 文件系统使用固定大小的簇. 我们常见的簇的大小通常是 4KB、8KB、16KB、32KB、64KB、128KB. 确定簇大小以后，所有文件的读写，都是按簇为单位进行统一分配. 比如说某个分区的簇大小为 32KB，一个 15KB 的文件，系统也会分配 32KB 的空间给它，但在这 32KB 的空间里边，真正被使用的只有 15KB，剩下的 17KB 是不能再分配给其他文件使用的. 这一部分的空间就是所谓的文件 SLACK 空间[1].

有两种类型的文件残留，一种是 RAM 残留(RAM Slack)，另一种是驱动残留(Drive Slack). RAM 残留是从文件的末端到最后一个所在扇区的末端，而驱动残留是从下一个扇区的开始到文件所在簇的最后一个簇的末端. 如图 4 所示:

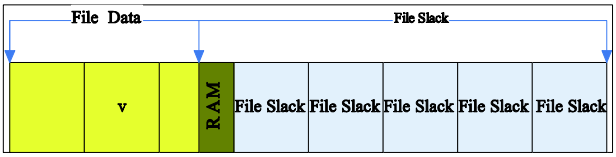

图 4 文件 Slack 结构图

由于 Windows 忽略存储在驱动残留中的信息，存储在该残留中的数据将不被操作系统本身检测. RAM

残留也能存储隐秘数据，但由于空间太小，往往不是理想的存储选择.

下面使用 Slacker.exe 工具向文件 Slack 空间写入数据. Slacker.exe 是一款可向 NTFS 文件系统的文件 Slack 空间写入数据的工具，以实现数据隐藏[3]. 用 Slacker.exe 把文件 test.txt(9 字节)写入图片文件 ptest.jpg 中，如图 5 所示:

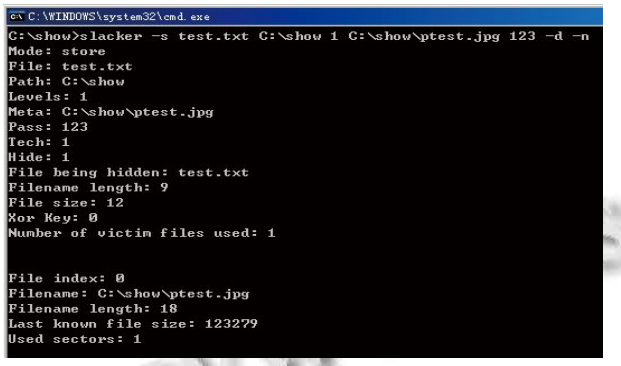

图 5　向一图片文件写入文本文件

成功写入数据后，使用 encase(4.0 版本)对 Ptest.jpg 文件写入前后进行分析比对(比对文件是生成的分析报告)，文件大小没有改变，但最后写入时间发生了变化. 同时，文件的其它属性也发生了很大的变化.如图 6 所示:

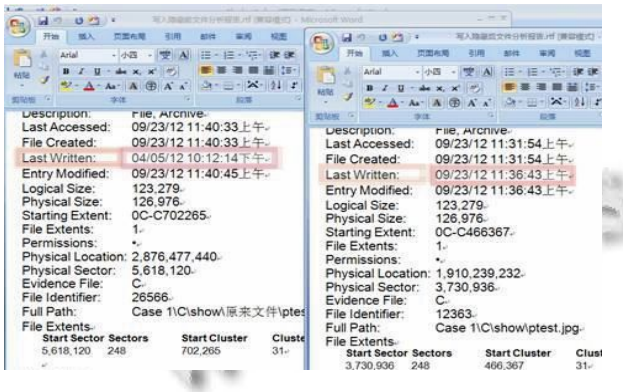

图 6　比较写入文件后图片文件的变化

3.5 分支数据流信息隐藏

分支数据流(Alternate Data Stream, ADS)是 NTFS 文件系统的一个特性，一种无须重新构建文件系统就能给文件添加额外属性或信息的机制. 允许单独的数据流文件存在，同时也允许一个文件附着多个数据流，即除了主文件流之外，还允许许多非主文件流寄生在主文件流之中，通过这种简单的文件流方式，可以实施文件隐藏[5].

由于针对 ADS 的取证分析工具很多，而且这种 ADS 数据隐藏方式健壮性较差，当将带有 ADS 文件流的文件拷贝到非 NTFS 分区时，此文件流会自动删除，如图 7 所示. 借助 ADS 流实施文件隐藏已经极为不可靠了.

图 7　将带有 ADS 文件流的文件拷贝到非 NTFS 分区时询问

3.6 NTFS 数据隐藏分析检测

分析 NTFS 数据隐藏一般是比较困难的，因为该文件系统非常灵活，可以支持各种操作系统，因此就会产生很多的数据隐藏方法. 另外，windows NTFS 文件系统的完整文件是保密的、不公开的，因此，有时无法判断在该文件系统数据结构中的值的组合，哪些是合理的，哪些是不合理的.

通常检查分析 NTFS 文件系统的隐藏数据可以分为三个阶段：检查确定是否有任何非正常数据隐藏；提取隐藏数据；覆盖隐藏数据.

对 NTFS 文件系统是否隐藏有数据，在每一次计算机取证过程中都要进行必要的分析. 一般来说，可以从如下几个方面来考虑. 一是在计算机取证分析之前，要对 NTFS 文件系统进行完整性检查，比如使用 chkdsk 命令行工具检查，出现的任何错误提示，就说明该文件系统或许存在被操纵的可能，而处于不稳定状态；二是检查文件被分配的簇的大小，与系统默认的该文件簇的大小(该大小是由文件本身的大小决定的)，一旦发现用户修改了该文件默认簇的大小，就说明是非正常现象，有可能通过修改默认簇大小以隐藏数据；三是在文件系统搜索数据隐藏工具；四是运用微软的 OEM 工具 NFI 检查元数据文件，NFI.EXE 是微软公司的 OEM 工具，用此工具可以转储 NTFS 主文件表的重要的元数据文件，也可以检查元数据文件的任何异常情况[5].

(下转第 37 页)

信息查询、票价信息查询、网上售票、自助取票等功能，极大的方便了乘客购票. 系统试运营以来，运行情况良好，能够在复杂因素的影响下保证售票的正常运行，具有广阔的应用前景. 当然也存在一些不足之处，比如不能直接在网上退票，还有系统安全方面的问题、容灾能力也需要进一步完善.

图 3 系统的购票界面图

图 4 班次确认界面图

参考文献

1 Horstmann CS, Cornell G.Java 核心技术.卷Ⅰ:基础知识 8 版.北京:机械工业出版社,2011.

2 reng10303,B/S 和 C/S 结构模式分析. [2008-06-05]. http://hi.baidu.com/reng10303/blog/item/464deceea81aclfeb3fb953c.html

3 胡孔法.数据库原理及应用.北京:机械工业出版社,2008.

4 李长河,赵杰,张亚玲,等.一种安全异构数据交换技术的研究与实现.计算机工程,2007,(2):88–89.

5 张军.异构数据源之间的数据转换方法.计算机应用,2005,(12):175–180.

6 章坚民,徐爱春,李海翔,等.基于 SVG/XML/CIM 的变电站自动化工程配置系统.电力系统自动化,2004,28(14):53–56.

7 Meng XN, Wang YB, Sun JR. Wireless data communication and applied foreground based on GPRS. Modem Electronic Technology, 2005(19):3l–33.

8 刘教瑜,吴美玲,谭杰.GPRS DTU 的设计及研究.电力自动化设备,2006(3):89–91.

9 黄文培.客票网上预订系统设计与研究.微电子学与计算机,2004,(7):21–25.

(上接第 4 页)

4 结语

数据隐藏技术一直以来就是计算机反取证重要技术之一，一切隐藏数据或通过隐蔽手段保护数据的措施和技术，都可以视为计算机反取证手段. 本文讨论的计算机系统的隐藏技术只是部分可能的隐藏数据的方法，随着技术的发展和新系统的产生，会有越来越多的数据隐藏方法出现，隐藏数据的艺术魅力主要还是依赖技术爱好者或嫌疑人的创造力. 更多的数据隐藏技术的创造和发现，可以有力的推进计算机取证技术的发展.

参考文献

1 Shin DM, Kim Y, Byun KD. Data Hiding in Windows Executable Files. Australian Digital Forensics Conference, 2008.

2 Gupta MR, Hoeschele MD, M.K.R. Hidden disk areas: Hpa and dco. International Journal of Digital Evidence, 2006,5(1).

3 Berghel.Hiding Data,forensics,and anti-forensics.Communications of ACM, 2007, 50(4):15–20.

4 李步升.基于 NTFS 的计算机反取证研究与实现.计算机工程,2010,36(19):274–276.

5 Huebner E, Bem D, Wee CK. Data Hiding in the NTFS File System. Digital Investigation 3, 2006: 211–226.